Beware Of The Phishers

infotextmanuscripts.org/djetc/av-phishers.html

elete
Move
Spam
Actions
Quota Exceeded
Sun, 2 Mar 2014 at 11:30
m BT - Broadband +
o a_baron@btinternet.com
s is to notify you that your mailbox limit has exceeded. Some messages(s)
t to your account will be rejected by our incoming mail server.
kÂ here to update your mailbox
to prevent your account from being permanently locked.
tomer Service
- Broadband

A screengrab of a phish e-mail. Whatever you do, do NOT “click here”.

Look at the screengrab above which arrived in a certain person’s inbox this morning, (apologies for the imperfect image which is caused by software limitations). Does this or does it not look like a genuine e-mail from an ISP? Yes, it does, but appearances can be deceptive. How can you tell? The very last thing you should do is click on the link indicated; that can be very expensive besides possibly damaging your computer.

With an e-mail like the above, if you have any suspicions at all, you can either ignore the message, or click on “show full headers”, copy and paste what you see, then paste that to an e-mail tracing tool like TraceAnEmail.com. This particular e-mail showed the following:

Email Source Analysis:

Sender: webmail.sysadm@bt.com

Source IP Address: 173.205.127.125

Source Host: ehub22.webhostinghub.com

Country: United States

State/Region:

City:

Latitude: 38.0000

Longitude: -97.0000

Why would British Telecom send an e-mail to a subscriber from the United States? Why indeed?

There are now all sorts of programs and tools you can use to protect your computer. If your machine is fairly new and you are running under Windows, the program will warn you when you are about to visit a “dodgy” site. There is the free Microsoft Security Essentials, and if you haven’t already invested in an anti-virus program, you can and should fit your machine with AVG, Norton or another top of the range product.

You can also find help on a dedicated anti-scam forum, many of which provide information about suspicious e-mails, websites and so on.

One of the most sophisticated scams employs direct human contact. You receive a telephone call from a lady with an exotic sounding accent who warns you personally, perhaps by name, that your computer has been infected by an extremely dangerous malware program; then she directs you to a website where you can download a program that will fix it. Tell her you are busy at the moment, ask her for her number and tell her you will call her back. Politely or otherwise, she will hang up.

The phishers are out there, and although both our computers and anti-malware programs are growing more sophisticated, they are doing their level best to stay one jump ahead. But there is no reason they should stay one jump ahead of you.

[The above article was first published March 2, 2014.]